IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

QVC, INC., **Plaintiff,** **v.** **RESULTLY, LLC,** **Defendant.**	**CIVIL ACTION** **NO. 14-6714**

OPINION

Before the Court is Plaintiff QVC, Inc.'s ("QVC") Motion for a Preliminary Injunction.[1] QVC asks the Court to enjoin Defendant Resultly, LLC ("Resultly") from "selling, divesting, licensing, distributing, transferring, removing, pledging, or otherwise disbursing" any of its non-cash assets during the pendency of this litigation. Mot. at 1. This request arises out of incidents in May 2014, when Resultly's web-crawling program overloaded QVC's servers, which rendered QVC's customers unable to access its website and resulted in substantial lost sales. Compl. ¶¶ 1-3. When Resultly learned of the problem from QVC, it immediately stopped the web-crawling activity and assured QVC that it would not restart. Opp. at 1. QVC agrees that Resultly is no longer crawling its site and does not suggest that Resultly is disingenuous in stating that it would not to do so again. It does, however, contend that Resultly is in a precarious financial position and, as such, may sell its intellectual property rights in its web-crawling program to a third party which could, in turn, use the program to cause harm to QVC's server. Mot. at 2-3. QVC's Complaint asserts a violation of the Computer Fraud and Abuse Act

[1] QVC also sought a temporary restraining order which the court denied on February 11, 2015 after full briefing and argument because QVC had not shown it would suffer irreparable harm absent the injunction.

("CFAA"), 18 U.S.C. § 1030(a)(5)(A), as well as a host of other state law claims under a variety of rubrics. Resultly argues that QVC is unlikely to succeed on the merits of its CFAA claim, that QVC will not suffer irreparable injury absent the requested relief, and that a preliminary injunction would result in greater harm to Resultly.

At the February 20, 2015 hearing to consider QVC's preliminary injunction, Resultly offered the testimony of Ilya Beyrak, Resultly's founder and CEO. QVC cross-examined Beyrak but declined to put on any of its own witnesses, relying instead on the affidavits of Randall L. Gainer, Sean Dwyer, and David Garozzo, and the arguments made in briefing. Based upon the parties' submissions, Beyrak's testimony, and oral argument, the Court denies QVC's motion for a preliminary injunction for the reasons set forth below.

I. BACKGROUND

A. *The Parties*

QVC is a "television and online retail giant" that markets and sells a wide variety of consumer products through live televised shopping programs, its websites, and other interactive media, including QVC.com. Mot. at 1; Gainer Decl. Ex. B at 2. In 2013, QVC reported that its e-commerce revenue was $3.2 billion—an average of around $8.7 million per day. Gainer Decl. Ex. B at 3.

Resultly is a four-year-old internet startup company that uses computer code to "crawl the web" to search hundreds of public websites of online retailers for the purpose of advertising to the public the merchandise of these entities in real time. Beyrak Decl. ¶ 3; Hr'g Tr. at 69:19-21. Resultly's intellectual property pertains to the method of choosing what information to crawl and extract from retailers' websites, and what information to display to users. Beyrak Decl. ¶ 8. It performs its crawling functions by utilizing and building upon open source software. Hr'g Tr.

at 24:15-25:12. Resultly hosts a consumer website and application that allows consumers to find products that are for sale, purchase them, and create and share collections with friends, peers, *etc*. *Id*. at 22:1-6. To illustrate, when a user on Resultly's webpage searches for a particular item, Resultly populates its page with items responsive to that search with product information it collects by crawling various retailers' websites. If a user wants to purchase any of those items, Resultly's webpage would take him or her directly to the retailer's website to complete the purchase. *See id.* at 32:6-15. Resultly views the service it provides as a benefit to both retailers and consumers. Dwyer Decl. Ex. A at 2. Recognizing this benefit, QVC allows many of Resultly's competitors, *e.g*., Google, Pinterest, The Find, and Wanelo, to crawl its website. Hr'g Tr. at 76:17-77:5. In fact, QVC has stated that its website is powerful enough to handle millions of such requests daily without issue. Mot. at 2 n.1.

B. *Resultly's Use of Open Source Software*

Resultly performs the crawling functions necessary to its business through a software program known as "abot." Beyrak Decl. ¶ 5; Hr'g Tr. at 24:12-25:12. The abot code is an open source C# ("C-sharp") web crawler, which means it is in the public domain on the Internet. Hr'g Tr. at 24:15-22. Resultly's software gives abot instructions on which websites it wants to crawl, as well as different configuration parameters, including whether Resultly wants to implement any "crawl delays," which control the speed at which Resultly's server pings a retailer's server with requests for information. *Id.* at 25:15-21. When abot returns pages that it crawls, Resultly processes that information through its own proprietary code. *Id.* at 25:8-12.

Even if Resultly does not sell its proprietary code, there is nothing preventing another company from using abot to crawl QVC's server in the same manner as Resultly. *Id.* at 25:22-

26:5. In fact, abot is the most popular crawler written in .NET and has been downloaded nearly 10 million times. *Id.* at 26:2-5.

C. *Resultly's Business Model*

Resultly's business model is dependent on the functional operation of retail websites that it crawls so as to maximize purchases made by customers who access those business websites through Resultly's website. Beyrak Decl. ¶ 9. Beyrak testified that Resultly's "purpose as a business is to find new products, find when products go on sale, and to provide that information to our users, who are people looking to purchase those types of items, and find new items that they have otherwise not found." Hr'g Tr. at 30:12-18. To achieve these goals, Resultly needs to maintain good relationships with retailers so that they do not block Resultly from crawling their websites. *See id.* at 41:5-15. Moreover, Resultly needs the retailers' websites to be functional so that its users can complete purchases of items they discover through Resultly. *See id.*

D. *Resultly's Business Plan*

Beyrak testified that Resultly's goal as of May 2014 was to produce a product and grow its user base. *Id.* at 30:22-31:2. When it accomplishes this goal, it will then seek to monetize that user base through advertising or some other mechanism. *Id.* at 31:3-5.

Meanwhile, Resultly currently makes money by collecting commissions on purchases made when a Resultly user clicks through Resultly's site to buy an item directly from a retailer. *Id.* at 31:6-15; 32:6-15. Resultly does not obtain the commission directly from the retailers whose sites it crawls. Instead, retailers such as QVC have an "affiliate" relationship with an intermediary company such as Commission Junction, whereby QVC pays the affiliate a percentage of the purchases made by users the affiliate brings to QVC's website. *Id.* at 73:12-74:24. Companies such as Commission Junction in turn enter into a contract with VigLink,

another intermediary that brings traffic to the affiliate retailers' websites by forming relationships with "publishers," *i.e.*, companies like Resultly that specialize in creating a user base of people who are looking to purchase products. *Id.* at 73:15-24.

In short, when a Resultly user buys a product on QVC, QVC pays a commission to Commission Junction (or a company in a similar affiliate position); Commission Junction then pays a share to VigLink; and finally VigLink pays a share of what it has received to Resultly. *Id.* at 72:20-74:24.

E. *May 2014 Events*

Resultly began crawling QVC's website in May 2014. For a certain period of time, Resultly crawled QVC's website for development purposes without complaint from QVC.[2] *Id.* at 26:13-27:12. Around May 9, 2014, Resultly began crawling the QVC website for production purposes. *Id.* at 26:13-20. On May 9 and 11, QVC's servers experienced an overload that impaired consumers' ability to use the site. Mot. at 1. QVC argues that the crash was caused because of the speed at which Resultly crawled its server. Compl. ¶ 14. QVC further argues that it was unable to quickly block Resultly's requests because Resultly had used IP addresses that were not identifiable as coming from a web-crawler. *Id.* ¶ 15.

At some point, presumably May 11, QVC was able to identify and block Resultly's IP addresses, which restored service to the QVC.com website. *See* Garozzo Decl. ¶ 11.

1. QVC's Relationship with Akamai

Requests for information and other content made to QVC.com from various internet users and software programs are routed through servers owned by Akamai Technologies, Inc. ("Akamai"). *Id.* ¶ 4. QVC uses a program called Akamai Security Monitor, including the

[2] Beyrak testified that Resultly had received complaints from smaller retailers in the past who had a problem with the speed at which Resultly crawled their website. Resultly had worked directly with those retailors to mitigate any problems. Hr'g Tr. at 70:4-8.

program's Web Application Firewall ("WAF") feature. *Id.* The WAF feature allows QVC operations specialists to set rules that are defined to warn and protect QVC.com from malicious requests. *Id.* ¶ 5. The Akamai servers are configured to cache certain content of the QVC.com website so that if the server has the requested content cached, Akamai can serve the response back to the requestor. *Id.* ¶ 6. If the response is not cached, Akamai will make a request to the QVC servers to obtain a response. *Id.* Akamai would then, based on defined caching rules, cache the response, and send the response back to the requestor. *Id.*

Due to QVC's relationship with Akamai, any request Resultly sent to QVC would actually hit Akamai's servers first. Hr'g Tr. at 29:10-13. If Resultly's question could be answered by the cached information on Akamai's server, Akamai would return the answer to Resultly. *Id.* at 29:21-30:3. If Akamai determined that its cached version was too out-of-date to answer the request, Akamai would then request the information from QVC's server. *Id.* at 71:6-72:4. When asked if he was aware of a risk of overloading QVC's site in spite of QVC's relationship with Akamai, Beyrak responded that he would not know the risk of overload because it would be "purely based on the configuration" between Akamai and QVC's server. *Id.* at 65:12-24.

2. Resultly's User Agent

A user agent is a "string" that is passed by a browser or other device, to a website, to identify what software is being used by that device to access the site. *Id.* at 35:12-23. Typically, Resultly includes the word "Resultly" at the end of its user agent string. *Id.* at 36:25-37:12. There is no requirement that Resultly identify itself this way. *Id.* at 82:12-16. However, Resultly wants to identify itself so as to "encourage retailers to participate on [Resultly's] platform." *Id.* at 36:25-37:12. At one point in 2014, likely including the period during which Resultly was crawling QVC's website, Resultly's user agent identification did not include the

word "Resultly." *Id.* at 36:17-24; 37:14-38:11. Beyrak testified that this was a mistake, and Resultly corrected the user agent to identify Resultly when it discovered the omission. *Id.* at 37:14-38:11.

QVC argues that because Resultly's user agent did not identify itself as a crawler, QVC believed that the requests were coming from individual customers instead of a bot. Garozzo Decl. ¶ 12. Beyrak testified that Resultly never attempted to mask or hinder identification of its IP addresses or bot. Hr'g Tr. at 38:14-16. Moreover, Beyrak testified that because Resultly's IP addresses are registered, QVC could have identified Resultly from its IP addresses either by referencing the American Registry of Internet Numbers ("ARIN"), by typing any of the IP addresses into address bar of a web browser, or conducting a "reverse look-up" of one of the IP addresses, which would have shown Resultly's name. *Id.* at 39:5-40:19. Beyrak testified that if QVC had used any of these methods, it would have immediately identified Resultly. *Id.* QVC could then either reach out to Resultly to request that it stop its activity, *id.*, or block Resultly by submitting a request to Akamai to create WAF rules blocking all requests coming from Resultly's IP addresses. *See* Garozzo Decl. ¶ 10.

3. Rate of Requests

QVC's Complaint alleges that Resultly "sent search requests on QVC's website at rates ranging from 200-300 requests per minute to up to 36,000 requests per minute, which overloaded QVC's website." Compl. ¶ 17. A letter from QVC's Assistant General Counsel, Vincent A. LaMonaca, to Beyrak states that the rate of requests coming from Resultly "approach[ed] 40,000 requests per minute." Gainer Decl. Ex. A. However, Beyrak testified that the maximum instructions that Resultly's server could send to QVC would likely be 10 to 20,000 per minute. Hr'g Tr. at 51:12-24.

Beyrak testified that the number of requests Resultly's server can send per minute is a function of the server's computing power, *i.e.*, the number of requests that its server can make, and the speed at which the server makes its requests. *See id.* at 56:24-57:4. The computing power of Resultly's server is fixed. *Id.* at 54:22-55:3. However, the speed at which Resultly's server can send requests depends upon whether or not the retailer has specified a crawl delay in a "robots.txt" file. *Id.* at 42:4-13. If a retailer has specified a crawl delay of twenty seconds, for example, Resultly's server will honor that standard and wait twenty seconds between requests, even if it has the capacity to send requests faster. *See id.* at 42:9-13. If the retailer has not specified a crawl delay, it was Resultly's practice in May 2014 that Resultly's server would send requests as soon as it received a response to its previous request. *Id.*

There is no industry standard that sets the outer limits of what a crawl rate should be. *Id.* at 66:6-11. Beyrak testified that the appropriate crawl rate for any particularly website would depend upon the circumstances and would take into account multiple factors, including "how many servers the company has, what technology they have, if the site is static or dynamic content, what language it's written in, how efficient it is, how many other requests they have coming in and whether those requests are coming from users or other bots." *Id.* at 49:22-50:4. When asked on cross examination what crawl rate Beyrak would suggest to QVC, Beyrak responded that he would need to know more information, but at a minimum, he would advise them to set the crawl delay for any unknown robots "to some high arbitrary number, in order to ensure protection." *Id.* at 50:17-24. Depending on the circumstances, Beyrak would sometimes suggest a crawl delay for a retail website at ten to twenty seconds. *Id.* at 51:1-11. Beyrak noted that a crawl delay of one second between requests is "super, super low." *Id.* at 66:15-18.

Beyrak testified that Resultly used one server to crawl QVC.com. *Id*. at 28:14-16. QVC does not specify a crawl delay through the robots.txt file. Mot. at 2; Garozzo Decl. ¶ 13. Thus, the speed at which the Resultly server operated depended on how quickly QVC's site responded. Hr'g Tr. at 28:21-24. QVC argues that it does not want to set a crawl delay because it wants to allow other web programs, such as Google, to crawl its websites. Garozzo Decl. ¶ 13. However, Beyrak testified that QVC had the ability to set a crawl delay for Resultly, or any other unknown crawler, independent of any delay that might set for another company such as Google. *Id.* at 79:22-80:7; 83:9-20.

F. ***Negotiations Between QVC and Resultly***

On May 28, 2014, QVC sent Resultly a cease-and-desist letter. Gainer Decl. Ex. A. The letter informed Resultly that its web-crawling activities overloaded QVC's servers by requesting information at a rate approaching 40,000 requests per minute. *Id.* Upon notification of a possible problem, Resultly immediately stopped crawling QVC.com and entered into negotiations with QVC. Beyrak Decl. ¶ 10.

On November 24, 2014, QVC filed its complaint against Resultly. QVC estimates that as a result of Resultly's web-crawling, it lost sales revenues of approximately $2 million, based on internal company estimates. Garozzo Decl. ¶ 15.

On November 25, 2014, Resultly's founder and CEO, Ilya Beyrak, wrote to QVC by e-mail stating that Resultly never intended to harm QVC's website. Dwyer Decl. Ex. A. Beyrak further indicated that it wished to resolve the dispute amicably due to limited funding. *Id*. In his email, Beyrak stated that Resultly's goal in crawling QVC's website was "to drive sales to [QVC] and provide a great service to our users in the process." *Id.* at 1. Beyrak further noted

that Resultly's software was designed to support the robots.txt standard for specifying a crawl delay; however, QVC's website did not specify a crawl delay. *Id.*

Negotiations continued until January 2015. Beyrak Decl. Ex. A. As part of the negotiations, Resultly provided QVC with a balance sheet showing its funding levels. Gainer Decl. Ex. D (filed under seal). QVC interpreted the balance sheet to show that Resultly's only asset of value was its proprietary code. Mot. at 3. As a result, QVC became concerned that Resultly would sell its software to a third party, which QVC believed would "pose a threat" to it and other website operators. *Id.* Accordingly, QVC filed its Motion for Temporary Restraints and Preliminary Injunction to enjoin Resultly from divesting its non-cash assets and thereby ensure that a third party will not acquire Resultly's software and use it to crawl QVC's server.

Because the Court finds that QVC is unlikely to succeed on the merits and has failed to show that it is likely to suffer irreparable harm in the absence of the injunctive relief it seeks, QVC's motion for preliminary injunction shall be denied.

II. LEGAL STANDARD

"A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). The "failure to establish any element . . . renders a preliminary injunction inappropriate." *NutraSweet Co. v. Vit-Mar Enters., Inc.*, 176 F.3d 151, 153 (3d Cir. 1999). The movant bears the burden of showing that these four factors weigh in favor of granting the injunction. *See Opticians Ass'n of Am. v. Indep. Opticians of Am.*, 920 F.2d 187, 192 (3d Cir. 1990).

III. DISCUSSION

A. *Likelihood of Success on the Merits*

As QVC did not premise its motion on any of its state law claims, it must show that it is likely to succeed on the merits of its CFAA claim. Section 1030(a)(5)(A) of the CFAA provides, in pertinent part, that whoever "***knowingly*** causes the transmission of a program, information, code, or command, and as a result of such conduct, ***intentionally*** causes damage without authorization, to a protected computer" has committed a federal offense. 18 U.S.C. § 1030(a)(5)(A) (2012) (emphases added). "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8). Here, Resultly does not contest that it "knowingly cause[d] the transmission of a program" to crawl QVC's website. *See* Gainer Decl. Ex. B at 2. However, Resultly argues that it has not violated subsection (a)(5)(A) because it did not "intentionally cause[ ] damage" to QVC's server. Opp'n at 7. Because "intentionally" is not defined by the statute, the issue the Court must decide is what level of intent is required to satisfy the *mens rea* portion of subsection (a)(5)(A).

1. The Scienter Requirement Under Section 1030(a)(5)(A)

In its opening memorandum, QVC argued that "only the intent to transmit a program to access the protected computer is relevant under the CFAA." Mot at 5. Resultly, noting QVC's reliance on an outdated version of the statute, responded that "the language of the statute requires (both allegation and proof) that the civil defendant: (1) knowingly causes the transmission of code; and (2) intentionally causes damage thereby." Opp'n at 5. At oral argument, QVC appeared to concede that subsection (a)(5)(A) requires intent to cause damage. *See* Hr'g Tr. at 7:8-13. However, QVC argued that such intent may be inferred through "objective indicators," such as expertise in coding, which show the defendant knew that its actions were likely to cause "some modicum" of damage to the plaintiff's computer. *Id.* at 7:20-8:3, 14:20-15:7. While

Resultly seemed to agree that a plaintiff could establish intent using circumstantial evidence, it argued that the relevant question is "whether Resultly was, in fact, sending out so much code that *anyone* would know it was going to impede QVC." *Id.* at 96:23-25 (emphasis added).

The Court finds that the plain language of the statute clearly requires that a Section 1030(a)(5)(A) defendant *both* knowingly transmit a code *and* intend to cause damage to the plaintiff's computer. This reading is consistent with the statute's legislative history and Third Circuit law. The Court further finds that while circumstantial evidence may be used to show intent, that evidence must show that it was the plaintiff's conscious objective to cause an "impairment to the integrity or availability of data, a program, a system, or information." Reckless or negligent behavior premised on the defendant's sophistication is insufficient. Finally, because the "objective indicators" QVC points to do not show that Resultly intended to cause *any* damage to QVC's server, the Court need not opine on whether Section 1030(a)(5)(A) requires that the defendant intended to create merely "a modicum" of harm or something more.

In evaluating the scienter required under Section 1030(a)(5)(A), the Court begins with the plain reading of the statute. Here, a plain reading of Section 1030(a)(5)(A) requires a dual standard of scienter: the defendant must *knowingly* transmit a code or command, and he must *intentionally* cause damage to the plaintiff's computer through this act. When a term in a statute is not defined, the Court looks first to how the Third Circuit has interpreted the term in the context of other cases involving the same statute. If the Third Circuit has provided no definitive interpretation of the provision at issue, this Court looks to the ordinary meaning of the words in the statute. *See United States v. Husmann*, 765 F.3d 169, 173 (3d Cir. 2014) (citing *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, 134 S. Ct. 1749, 1755 (2014)). In addition, it is helpful to look at the statute's legislative history to see if any light can be shed on the meaning of

the undefined term. *See, e.g.*, *Menkowitz v. Pottstown Mem'l Med. Ctr.*, 154 F.3d 113, 118 (3d Cir. 1998).

a. *Plain Meaning*

Again, Section 1030(a)(5)(A) provides that a defendant has violated the CFAA if it "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A) (emphasis added). The Oxford English Dictionary defines "intentionally" as to act "with intention, on purpose." *Intentionally*, Oxford English Dictionary (2015), http://www.oed.com/view/Entry/97497. "Purpose" is defined as "by design, as opposed to by chance or accident." *Purpose*, Oxford English Dictionary (2015), http://www.oed.com/view/Entry/154972. Black's Law Dictionary defines "intentional" as something that is "done with the aim of carrying out the act." Black's Law Dictionary 932 (10th ed. 2014). Thus, under a plain reading of Section 1030(a)(5)(A), the plaintiff must show that a defendant acted "on purpose" or "with the aim" to "impair[ ] the integrity or availability of data, a program, a system or information."

Although the Court finds that the statute clearly imposes an intent requirement with respect to the damage clause, the Court acknowledges some ambiguity as to whether the "as a result of" clause suggests that if a defendant knowingly sends a computer code to a protected computer, that *itself* is sufficient to show that the defendant intended to cause the damage. To resolve this ambiguity, the Court next turns to the statute's legislative history.

b. *Legislative History*

A review of the legislative history of the statute makes clear that, in its current form, Congress intended for subsection (a)(5)(A) to require both that the defendant *knows* he

transmitted a code or program to a protected computer and *intended* for that code or program to cause damage.

The CFAA was first enacted in 1984 to prohibit harm caused by unauthorized access to "federal interest computers," defined as governmental and financial institution computers. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 1837 (codified as amended at 18 U.S.C. § 1030) [hereinafter "1984 Act"]. The 1984 Act made it a felony to knowingly access classified information from a federal computer without authorization, and a misdemeanor to access financial records or credit histories in financial institutions, or to trespass into a government computer. Subsection (a)(3) covered anyone who:

> ***knowingly*** accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct ***knowingly*** uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of United States and such conduct affects such operation.

Id. Notably, the 1984 Act contained a dual *mens rea* requirement, *i.e*., the defendant must act "knowingly" with respect to *both* "access[ing]" a federal computer *and* "us[ing], modif[ying], destroy[ing], or disclos[ing]" information gained through such access.

In 1986, Congress revised the Act in light of a growing concern about computer crime. *See* S. Rep. 99-432 (1986). The 1986 amendment cleaned up ambiguities in the original statute, created a more coherent structure of offenses, and expanded the scope of the Act to encompass additional types of computer crime. It added three new offenses, including a hacking offence, subsection (a)(5), which penalized those who:

> ***intentionally*** access[] a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby . . . causes loss. . .

Computer Fraud and Abuse Act, Pub. L. No. 99-474, § 2, 100 Stat. 1213 (1986). Like the original statute, this version of the statute was intended to reach "outsiders," *i.e.*, those, such as hackers, "lacking authorization to access any Federal interest computer." S. Rep. 99-432, at 10. Its *mens rea* requirement included an "intentionality" component, a higher requirement than the "knowingly" requirement used throughout the original statute. Following the 1986 amendment, there was some confusion as to whether "intentionally" applied to both the "access" clause and the "damage" clause of the statute, or whether the *mens rea* requirement only applied to the first clause. In *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), the Second Circuit concluded that a defendant could be convicted so long as the evidence showed that he intentionally accessed a Federal interest computer without authorization and that damage was caused by this access. The court noted that, unlike the original statute, the 1986 version did not repeat the *mens rea* requirement after the "access" phrase, whereas other subsections retained this dual-intent requirement. *See id.* at 508.

In 1994, subsection (a)(5) was rewritten to create two new offenses that brought back a dual-intent requirement. The first offense covered intentional acts, which remained a felony, and the second created a misdemeanor for merely reckless acts. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, § 290001, 108 Stat. 1796. Moreover, Congress expanded the scope of subsection (a)(5) from federal interest computers to any "computer used in interstate commerce" and did away with the requirement that the defendant lack authorization to access the protected computer. *Id.* Specifically, subparagraph (5)(A) provided, in pertinent part, that whoever:

> through means of a computer used in interstate commerce or communications, ***knowingly*** causes the transmission of a program, information, code, or command to a computer or computer system if—
>
> (i) the person causing the transmission ***intends*** that such transmission will

> (I) damage, or cause damage to, a computer, computer system network, information data, or program; or
>
> (II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program; and
>
> (ii) the transmission of the harmful component of the program, information, code or command—
>
> (I) occurred without the authorization of the person or entities who own or are responsible for the computer system receiving the program, information, code, or command; and
>
> (II) (aa) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1- year period; or (bb) modifies or impairs . . . medical care of one or more individuals.

Id. (emphasis added). By moving the "without authorization" clause to the damage section, Congress intended to capture Federal employees or other "insiders" who generally were authorized to access Federal computers but exceeded their authority by causing damage to the system. *Id.*

In 1996, Congress completely restructured subsection (a)(5), creating three offenses: two felonies and one misdemeanor. Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201, 110 Stat. 3488. Congress changed the Act to cover a wide range of crimes and applied a different *mens rea* to each offense. *Id*. Together, these subsections criminalize the actions of anyone who:

> (5)(A) ***knowingly*** causes the transmission of a program, information, code, or command, and as a result of such conduct, ***intentionally*** causes damage without authorization, to a protected computer;
>
> (B) ***intentionally*** accesses a protected computer without authorization, and as a result of such conduct, ***recklessly*** causes damage; or
>
> (C) ***intentionally*** accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

Id. § 201(E) (emphases added). In all three subsections, the defendant must either knowingly or intentionally access a protected computer. However, each subsection requires a *different mens rea* with respect to damage. The first offense, codified in subsection (a)(5)(A)—and relied upon by QVC here—is the only subsection that applies to "insiders"—*i.e.*, defendants who generally have permission to access the protected computer but who have exceeded their authority by transmitting a program or code that harms the protected computer. Thus, subsection (A) requires that the defendant intend to cause the damage that occurred. By contrast, subsections (B) and (C) apply to "outsiders"—*i.e.*, defendants who do not have authority to access the protected computer. Subsections (B) and (C) require an intent to trespass creating a violation if the action even recklessly or negligently causes damage to a protected computer.

The Senate Report for the 1996 amendment discusses the rationale for the layered *mens rea* requirements, stating: "In sum, under the bill, insiders, who are authorized to access a computer, face criminal liability *only if they intend to cause damage to the computer*, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass." S. Rep. 104-357, at 11 (1996). The report continues:

> The rationale for this difference in treatment deserves explanation. Although those who intentionally damage a system, without authority, should be punished regardless of whether they are authorized users, it is equally clear that anyone who knowingly invades a system without authority and causes significant loss to the victim should be punished as well, even when the damaged cause is not intentional. In such cases, it is the intentional act of trespass that makes the conduct criminal. To provide otherwise is to openly invite hackers to break into computer systems, safe in the knowledge that no matter how much damage they cause, it is no crime unless that damage was either intentional or reckless. Rather than send such a dangerous message (and deny victims any relief), it is better to ensure that section 1030(a)(5) criminalizes all computer trespass, as well as intentional damage by insiders, albeit at different levels of severity.

Id.

Since 1996, Congress has amended the CFAA multiple times but has not altered the dual *mens rea* requirements set forth in subsections (A)–(C) above. It is clear, therefore, that "knowing transmission" of a code to a protected computer does not imply "intent to cause harm." Rather, if a plaintiff proceeds under Section 1030(a)(5)(A), it must show that the defendant intended to cause harm to plaintiff's computer through its access. Damage caused by mere recklessness or negligence is insufficient.

c. *Case Law*

The Third Circuit has defined "intentionally" in the criminal context as performing an act "deliberately and not by accident." *United States v. Carlson*, 209 F. App'x 181, 184 (3d Cir. 2006) (citing *United States v. Barbosa*, 271 F.3d 438 (3d Cir. 2001)). Applying this definition in the context of a Section 1030(a)(5)(A) case, a panel of the Third Circuit held that a violation occurs if it was "the defendant's *conscious objective*" to cause harm to a protected computer. *Id.* at 184-85 (emphasis added). In other words, a plaintiff alleging a Section 1030(a)(5)(A) violation is "required to prove at trial that [the defendant] deliberately caused an impairment to the integrity or availability of data, a program, a system, or information." *Id.*

QVC urges the court to read *Carlson* and a follow-up case, *United States v. Prugar*, No. 12-267, 2014 WL 4716382 (M.D. Pa. Sept. 22, 2014), to hold that: (a) a plaintiff need not show that the defendant acted with malice but merely an intention to cause damage as defined by the statute; and (b) defendant's intent may be inferred from circumstantial evidence. Specifically, QVC interprets *Carlson* and *Prugar* to hold that a defendant's intent to cause harm can be circumstantially inferred from outward identifiers.

In *Carlson*, the defendant was alleged to have sent thousands of emails to specific email addresses, typically belonging to journalists or members of the Philadelphia Phillies, as an attempt to draw attention to issues he considered important. For example, the defendant sent

5,000 emails to a member of the Phillies with the subject line "Sign JASON GIAMBI." The defendant denied any intent to cause damage to the individual e-mail accounts. However, at trial, Carlson admitted that when he sent thousands of e-mails to a single address, "the targeted inbox would flood with e-mails and thus impair the user's ability to access his other 'good' emails." 209 F. App'x at 183. The court concluded that "Carlson's level of internet savvy, combined with his actions, could rationally be used to conclude that Carlson intended the consequences of his actions." *Id.* at 185.

In *Prugar*, the defendant gained unauthorized access to his previous employer's servers in order to retrieve certain data. After locating the data, the defendant created a script to delete log files showing his actions. Although the defendant stated he did not intend to harm the employer's computer, his act of deleting log files squarely caused "damage" under the CFAA because it "impair[ed]the integrity or availability of . . . information" on the employer's network. Thus, the court found that the evidence established defendant's intent to harm even if "his deliberate deletion of [the logs] was done with the purpose of concealing his access rather than causing the system to malfunction or pecuniary harm." 2014 WL 47166382, at *10.

The Court agrees that *Carlson* and *Prugar* support QVC's contention that a Section 1030(a)(5)(A) plaintiff may use circumstantial evidence to infer intent to cause damage—"damage" being statutorily defined as "any impairment to the integrity or availability of data, a program, a system or information." 18 U.S.C. § 1030(e)(8)(A). However, it is still unclear what specifically the circumstantial evidence would need to show. On one end of the intent spectrum, the plaintiff may need to show that the defendant acted with malice, *i.e.* a deliberate desire to harm the plaintiff's computer. On the other end, a plaintiff may only need to show something akin to (but more than) recklessness, *i.e.*, that an external observer would say

that someone with the defendant's level of expertise *should have known* that harm was likely to occur. At oral argument, the Court asked QVC where it believed the line should be drawn. Counsel for QVC urged the Court to draw the line "in the middle somewhere" such that the defendant "intended to have *some* impact." Hr'g Tr. at 14:20-15:7 (emphasis added). In other words, a defendant need only "intend[ ] to do some modicum of harm" regardless of whether the defendant intended the full impact of his actions. *Id*. at 14:20-15:7.

Without deciding the precise point on the continuum necessary to establish intent, the Court finds that the "objective indicators" plaintiff points to do not show that it was Resultly's conscious objective to cause "impairment to the integrity or availability of" information on QVC's server – even "some modicum" of harm.

2. No Evidence of Intent to Harm

Here, QVC argues that there are two objective indicators of Resultly's intent to cause damage to QVC's servers: (1) the "astounding" speed at which Resultly crawled QVC's server; and (2) the fact that Resultly did not identify itself as a bot in its user agent, which caused QVC to interpret Resultly's requests as coming from individual users. *Id.* at 8:12-18. Even accepting these facts as true, the weight of the evidence clearly shows that Resultly did not intend to harm QVC's server. Beyrak offered compelling and credible testimony that it would have been antithetical to Resultly's business goals to render QVC's server unavailable to customers. *See id*. at 41:2-15. As a growing start-up, Resultly was attempting to form positive business relationships with the retailers whose websites it crawled, not alienate them. *See id.* at 41:19-23 ("Our business relies on being able to both access . . . content from retailers, as well as getting retailers on board with our platform as we move further, and having users ultimately make purchases on those sites."). In addition to avoiding costly litigation, Resultly had numerous business reasons not to harm a retailer's site. For example, Beyrak testified that if Resultly

harmed a retailer's website, the retailer would typically block Resultly, which would prevent Resultly from showing that retailer's products on its own site. *Id.* at 41:7-11. Moreover, if a Resultly user decided to buy a product from a retailer's site and was redirected to that site to make the purchase, it would be contrary to Resultly's interests if the retailer's website did not function properly or was slow. *Id.* at 41:12-15.[3]

Because it was Resultly's objective to have QVC's site operating in conjunction with Resultly's own service, it would be inappropriate to infer, as in *Carlson*, that Resultly knew it would cause damage to QVC's server but went ahead with its actions anyway. Rather, the evidence suggests that if Resultly knew it would have damaged QVC's computer, it would not have engaged in the conduct. And unlike the defendant in *Prugar*, Resultly did not intend to damage Resultly's computer in a statutory sense as, again, "impair[ing] the integrity" of QVC's server would *frustrate*, rather than promote, Resultly's main objective to "drive sales to retailer[s] and provide a great service to [its] users in the process." Dwyer Decl. Ex. A.

The Court also notes that representatives from both QVC and Resultly stated that Resultly's crawling code was actually directed at Akamai, not QVC. QVC employee David Garozzo's declaration acknowledges that QVC did in fact retain Akamai, and that in fact, when QVC ultimately blocked Resultly, they did so by instructing Akamai to implement the block. Garozzo Decl. ¶¶ 8-11. Beyrak offered oral testimony—to which QVC did not object—that, "from what he has read," QVC retained Akamai for caching and other functions, *id.* at 29:10-13, and that when Resultly crawled QVC's webpage, it was actually crawling Akamai's server. *Id.* at 30:4-11. If Resultly knew of QVC's relationship with Akamai prior to May 2014, QVC would

[3] Resultly benefits when its users purchase products they find on retailers' sites in two ways: first, a sale would, theoretically, make Resultly's user happy and build loyalty to the Resultly website; and second, Resultly would receive a commission on the sale. *See generally* Hr'g Tr. at 30:23-31:15.

be hard pressed to prove that Resultly intended to cause damage to QVC's server by accessing Akamai's server.

In any event, Resultly was not QVC's competitor, a disgruntled QVC employee, or an unhappy QVC customer aiming to cause damage to QVC's server. To the contrary, Resultly's goal was to grow a loyal user base of people who gain something from being directed to QVC's website. For Resultly to meet this goal, it needed the QVC website to run smoothly, and it needed QVC to allow Resultly to crawl its site. Although Resultly may have ultimately damaged its relationship with QVC by: (1) assuming that QVC's website could handle Resultly's requests without implementing a crawl delay; and (2) failing to identify itself in its user name during the time it crawled the QVC server, neither of these "objective identifiers" suggests that Resultly wanted to damage QVC's server or thought damage was a likely outcome of its actions.

a. *Crawl Rate*

QVC's first "objective indicator" of Resultly's intent to harm QVC's servers is the "astounding crawl rate of 40,000 hits per minute." *Id*. at 8:12-14. Although the parties disagree as to the exact rate at which Resultly crawled QVC's website,[4] the Court finds that the exact rate is irrelevant given Beyrak's testimony that Resultly crawled the QVC website in the same manner as it crawled any other website that did not provide a robots.txt file specifying a crawl delay. Beyrak testified that the rate of Resultly's requests depended upon whether the retailer

[4] The only evidence in the record that the crawl rate hit 40,000 requests per minute comes from a May 28, 2014 letter from QVC's Assistant General Counsel, Vincent A. LaMonaca, to Resultly's CEO, Ilya Beyrak, which states: "QVC is informed and believes that for extended periods of time on May 9 and again on May 11, crawling activities originating from IP addresses associated with Resultly occurred on qvc.com. These activities included scripts containing an unreasonably high rate of requests—*approaching 40,000 requests per minute*." Gainer Decl. Ex. A (emphasis added). However, Beyrak testified that, given Resultly's server capacity, the maximum speed at which it could have crawled QVC's server would have been around 10 to 20,000 requests per minute. Hr'g Tr. at 51:18-24. QVC did not offer any oral testimony to dispute Beyrak's assessment.

had set up a robots.txt file with a crawl delay and, if not, the speed at which the retailer's server could respond to Resultly's requests. Beyrak stated:

> [On] May 9th of 2014, the way it would set its rates is it would look at the robots.txt file that's provided by the destination site, and see if that site has requested a crawl delay. If they have, we follow that standard, which is more a courtesy than the rule. If they have not, that machine will attempt to crawl their site and basically as quick as it can, and as quick as the site responds.

See id. at 42:4-13. For the past four years, Resultly has been crawling hundreds of retailers' sites. *Id.* at 69:19-21. During this time, Resultly had never been told by a large company such as QVC that its crawl rate was too high. *Id.* at 68:25-70:20, 89:7-90:10. There is therefore no evidence on this record that Resultly was on notice that its system of sending requests as fast as it receives a response was likely to cause damage to QVC's server.

Moreover, Resultly relied upon QVC to specify a crawl delay if it could not handle a high volume of requests. In Beyrak's experience, "every major retailer who [sic] [Resulty] has encountered has a proper throttle set." Gainer Decl. Ex. B at 3. In an affidavit, a QVC employee, David Garozzo, testified that Beyrak advised QVC at some point after the May 2014 incidents that harm to its server could have been avoided if QVC had implemented a crawl delay in a robots.txt file. Garozzo Decl. ¶ 13. QVC argues that it would be unreasonable to implement a crawl delay because it would slow down their system too dramatically given that QVC already supports "millions of page crawls" by other companies like Google. *Id.* However, Beyrak testified that this is a non-issue given the flexibility allowed in a robots.txt specification. Beyrak explained:

> [T]he robots.txt specification allows you to set completely different and arbitrary rules that are different for every single piece of software. So you could set one delay for Google, you could set a different one for Yahoo, a different one for Resultly, not only as far as the crawl delay but on which page it should crawl, or to crawl on no pages, for that matter. Or it could specify a rate for Google and another rate for any unknown bots.

Hr'g Tr. at 79:14-21. QVC provided no evidence to refute this point.

Because Resultly's crawl rate was implemented according to procedures that had been in place for a period of time and had never caused a problem, and because QVC could easily have implemented a crawl delay for unknown bots while still allowing the programs it wants to crawl its site to do so at higher speeds, the Court finds that Resultly's crawl rate is not an "objective identifier" that can support an inference of intent to harm.

b. *User Agent Identifier*

QVC argues that intent to harm QVC's server can also be inferred from the fact that Resultly's user agent identifier did not identify itself as a bot, leading QVC to believe that the requests were coming from individual customers rather than a web crawler. *Id*. at 8:15-18. QVC argues that Resultly "masked" its identity in order to confuse QVC, presumably in order to prevent QVC from effectively stopping its activity. *Id.* at 9:9-23.

Beyrak testified that Resultly never attempted to hide its IP addresses. *Id.* at 39:2-4. Moreover, Beyrak's testimony showed that, far from trying to hide its identity, Resultly actively identified itself to the retailers whose sites it crawled. *See id.* at 37:2-7 ("It's included in there, so that—to basically show whoever['s] site we're crawling if they look at their logs who we are, and that we're, you know, representing who we are, and that's the only way for us to really pass our company information along to them.") When asked why Resultly wanted to pass its information along to retailers, Beyrak stated: "Because especially as we've grown now, we encourage retailers to participate on our platform, and because we have no reason to hide who we are." *Id.* at 37:10-12. Beyrak explained that at some point in time, Resultly's name did not appear in its user agent, but that this was a mistake. *Id.* at 37:14-38:11. Resultly corrected the issue after a retailer with whom Resultly has a good relationship informed Beyrak that that there was a problem. *Id.* The Court has no reason to doubt Beyrak's testimony.

Further, Resultly's IP addresses all came from the same block, as opposed to a random set of IP addresses that would be more easily confused with coming from the public at large. Beyrak Decl. ¶ 4. Garozzo's affidavit corroborates Beyrak's testimony. He states:

> An inspection of the request origin webserver logs revealed a large number of unique requests that all contained an unusually high number of search attributes, which is what was causing the requests to require back-end processing on QVC's servers. These requests all came from within the IP block range of 23.29.132.0/23. This high volume of requests—hundreds of IP addresses, all from the identified IP block range, making simultaneous, distinct requests—had the effect of a distributed denial-of-service attack and caused QVC.com to become unable to process customers' legitimate requests. Upon recognizing the pattern of requests coming from the IP block range of 23.29/132.0/24, QVC submitted a request to Akamai to create WAF rules blocking all requests coming from the identified range of IP addresses. Immediately after the block was implemented, the QVC.com website returned to normal, stable operations. The block remains in effect today.

Garozzo Decl. ¶¶ 8-11. Garozzo's declaration does not explain why it took QVC until May 11 to recognize that the requests originated from the same IP block range. QVC did not offer any testimony to explain why the "inspection of the request origin webserver logs" did not occur immediately after QVC.com began to experience issues, or to otherwise explain why QVC did not immediately put a block in place. Beyrak testified that there were at least three ways in which QVC could quickly have identified the IP addresses as belonging to Resultly: *first*, QVC could have looked up one any of the IP addresses in the ARIN database; *alternatively*, QVC could have copied and pasted any of the IP addresses into a browser, which would have pulled up Resultly's website; *finally*, QVC could have run a "reverse look-up" of Resultly's IP addresses and discovered that they came from Resultly. Hr'g Tr. at 39:5-40:10. There is no evidence that QVC tried any of these methods.

Given Resultly's undisputed testimony about its typical practice of including its name in its user agent, the fact that QVC identified Resultly's requests as belonging to the same IP block, and the ease with which QVC could have identified the IP addresses as originating from

Resultly, the Court finds that Resultly's failure to identify itself as a bot in its user agent cannot be used to infer an intent to cause damage to QVC's server.

B. *Irreparable Harm*

Although the Court need not address any of the remaining factors for a preliminary injunction as "failure to establish any element . . . renders a preliminary injunction inappropriate," *NutraSweet Co.*, 176 F.3d at 153, the Court finds that denial of QVC's motion is also warranted because QVC has failed to demonstrate a likelihood of irreparable harm.

QVC offers two arguments in support of its claim of irreparable harm. *First*, it opines that "[i]f Resultly assigns the software code unaltered to another company, the same mischief QVC seeks to protect itself against will likely occur again." Mot. at 6. This argument makes little sense in light of Beyrak's testimony that Resultly used open source software – available free to anyone – to crawl QVC's website and the fact that QVC has the ability to *prevent* any unwanted crawling of its site. As noted above, Beyrak testified that Resultly's intellectual property works in tandem with open source software to specify the information Resultly wants to extract from retailers' websites and display to users. Beyrak Decl. ¶ 8. Resultly's proprietary code also enables Resultly to implement a crawl delay, which *slows down* the crawl rate inherent in the open source code. Hr'g Tr. at 25:15-21. As Beyrak testified, anyone wanting to crawl QVC's website at a high speed is already able to do so whether or not Resultly sells its proprietary software. *Id.* at 25:22-26:5. And even if Resultly's software *could* enable a third party to crawl the QVC server at a faster speed than the open source software already allows, Beyrak testified that QVC can easily prevent another crash by specifying a crawl delay for any unknown bots in a robots.txt file. *Id.* at 79:14-21. Moreover, QVC can do so without limiting the rate for web-crawlers it prefers, such as Google. *Id.* QVC is therefore perfectly able to

protect itself from harm without resort to an "extraordinary remedy" such as a preliminary injunction, "which should be granted only in limited circumstances." *Novartis Consumer Health, Inc. v. Johnson & Johnson-Merck Consumer Pharm. Co.*, 290 F.3d 578, 586 (3d Cir. 2002) (quotation marks omitted).

Second, QVC argues that a preliminary injunction is necessary to "protect [QVC's] potential future damages remedy" due to a concern that if Resultly sells its non-cash assets it will be rendered judgment-proof. Mot. at 7. Citing *Hoxworth v. Blinder, Robinson & Co., Inc.*, QVC notes that a Court may protect a future damages remedy if the plaintiff shows: (1) that it is "likely to become entitled to the encumbered funds upon final judgment"; and (2) that "without the preliminary injunction, plaintiff[ ] will probably be unable to recover those funds." 903 F.2d 187,197 (3d Cir. 1990). Here, QVC has failed to establish the first *Hoxworth* requirement because, as addressed in Section A above, the Court finds that QVC is unlikely to succeed on the merits of its CFAA claim—the only claim upon which QVC brings its Motion. It is therefore is not entitled to equitable relief under *Hoxworth.*

QVC also cites *Elliott v. Kiesewetter*, which held that, consistent with *Hoxworth*,

> a court may find that a party seeking an asset freeze to preserve a money judgment may show irreparable injury by showing that the freeze is necessary to prevent the consumption, dissipation or fraudulent conveyance of *the assets that the party pursuing the asset freeze seeks to recover in in the underlying litigation.*

98 F.3d 47, 58 (3d Cir. 1996) (emphasis added). As an initial matter, a plaintiff seeking equitable relief under *Elliot* would still need to satisfy the *Hoxworth* requirements, which QVC has failed to do. Moreover, in *Elliot*, the property assets plaintiffs sought to freeze were the very assets plaintiffs sought to have returned to them at the conclusion of the case. For that reason, the Third Circuit found that the "equitable nature of the [plaintiffs'] desired relief offers an additional compelling justification" for upholding the district court's grant of a preliminary

injunction. *Id.* Here, QVC does not seek to acquire title to Resultly's code; it simply seeks monetary damages. Thus, the Court finds that *Elliot* is equally unavailing to QVC.

IV. CONCLUSION

To show a likelihood of success on the merits of its CFAA claim, QVC must show that when Resultly crawled QVC's website, it intended to cause damage to QVC's server. However, the evidence introduced at this stage in the proceedings overwhelmingly shows that Resultly had no incentive or desire to cause QVC's webpage to slow down, let alone overload. To the contrary, Resultly's business plan requires that the websites it crawls stay functional. At most, the objective indicators QVC offers regarding Resultly's crawl speed and user agent information suggest that, as a fledgling company, Resultly had yet to iron out certain wrinkles in its business operations. While Resultly's conduct may be sufficient to demonstrate negligence or recklessness, the Court cannot infer that Resultly *intended* to cause damage to QVC's servers as required by Section 1030(a)(5)(A).

Furthermore, QVC has failed to show a likelihood of irreparable harm in light of Beyrak's testimony about the role of open source coding in Resultly's web-crawling and QVC's undisputed ability to protect itself against any future outages caused by unknown bots. Accordingly, the Court shall deny QVC's request for a preliminary injunction.

An appropriate Order follows.

BY THE COURT:

/S/WENDY BEETLESTONE, J.

WENDY BEETLESTONE, J.

Dated: **March 13, 2015**